

Appendix A. Implementation Details of Strong Authentication at Fermilab

In this appendix we discuss the concept of strong authentication and the features and environment as implemented at Fermilab.

A.1 What is “Strong Authentication”?

A.1.1 Definition

A succinct definition of strong authentication was given by Tardo and Alagappan¹:

“Techniques that permit entities to provide evidence that they know a particular secret without revealing the secret.”

In more practical terms, it is a system of verifying workstation user and network server identities on an unprotected network in which the parties must demonstrate knowledge of a “secret” rather than transmit a password. Typically the verification is done via a trusted third-party authentication service using conventional cryptography. Strong authentication avoids relying on authentication by the host operating system or basing trust on host addresses. It does not require that the network be safe from eavesdropping, or from injection of hostile packets or alteration/deletion of packets².

A.2 Goals of Strong Authentication at Fermilab

Fermilab must demonstrate to the DOE that it is implementing a computer security system that exercises tight control over who uses the lab’s computers and network (which are owned by the government). The Computing Division has been charged with implementing Strong Authentication to meet Fermilab’s obligation.

1. J.J. Tardo and K. Alagappan, “SPX: Global Authentication Using Public Key Certificates.” In *Proc IEEE Symp. Research in Security and Privacy*. IEEE CS Press, 1991.

2. The Kerberos authentication process can fail if too many packets are altered or deleted (e.g., all of them in one or both directions, until the client gives up).

A primary goal of this effort is to essentially eliminate the transmission of clear text reusable passwords over the network and their storage on local systems. It is impossible to entirely prevent the transmission of clear text passwords, but we are implementing a solution that removes the most common opportunities as well as most of the necessity for typing a password.

Other important goals for us include:

- Providing a single sign-on environment for users
- Providing access to users who have no specialized software (this necessitates an unencrypted mode of access)
- Integrating existing accounts
- Centralizing account maintenance
- Consistently enforcing password policies such as length, quality and lifetime

A.3 The Authentication Model Implemented at Fermilab

The strong authentication service implemented at Fermilab is the Kerberos Network Authentication Service V5. We describe many of its features in Chapter : *About the Kerberos Network Authentication Service V5*. In this section we describe the model more generally.

A.3.1 The Realms

The model employed at Fermilab divides the computing environment into three *realms*:

The strengthened realm

The strengthened realm consists of all systems (whether on- or off-site) that require strong authentication for access from the network. On a strengthened system, all traditional means of access that use weak authentication, such as **telnet**, **rlogin**, **FTP**, and so on, are replaced with strengthened versions of these programs. Means of access over the network that do not involve passwords are allowed. Weak authentication (standard security) is allowed for local access only, i.e., via the console or locally attached display.

The production realm at Fermilab for UNIX machines is called FNAL.GOV¹, and for Windows 2000, there is FERMI.WIN.FNAL.GOV.

The trusted realm

Other sites which implement strong authentication, and which meet certain criteria, may be recognized by the strengthened realm at Fermilab as a “trusted” realm. Trusted realms provide levels of security and authentication equivalent to our own. Trust relations (cross-authentication) between the trusted realm and the strengthened realm allow access without further authentication (i.e., the authentication takes place only when user accesses either realm individually).

The untrusted realm

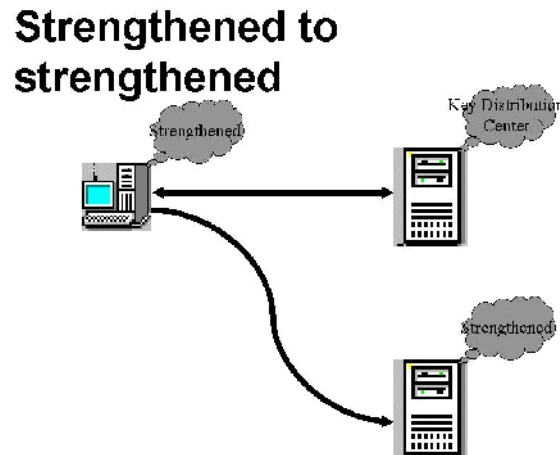
1. As long as the PILOT.FNAL.GOV realm is operating in parallel, the information in this manual applies equally to both realms.

The untrusted realm consists of those systems that do not require strong authentication and that permit traditional means of access. These systems typically expose clear-text passwords on the network.

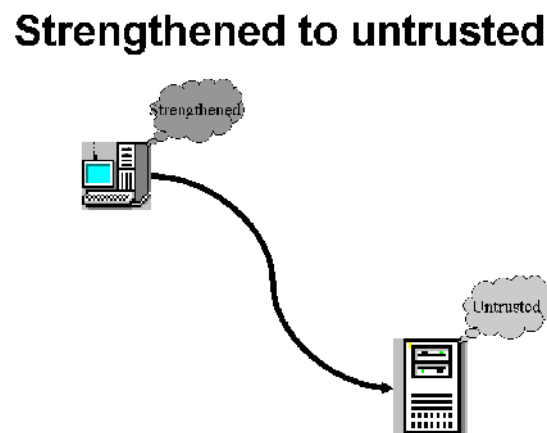
A.3.2 Relationships between the Realms

The figures below illustrate the relationships between these realms. (The Key Distribution Center, or KDC, shown on these figures is described in Chapter : *About the Kerberos Network Authentication Service V5.*)

Direct connections between machines in the strengthened realm are allowed



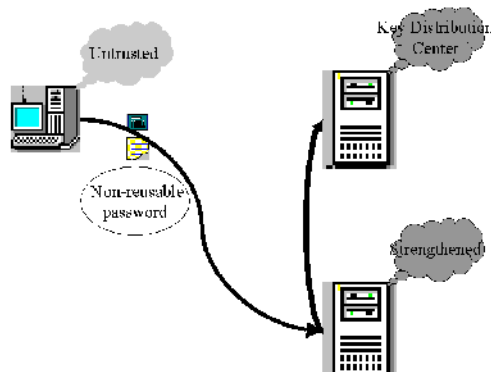
(the Key Distribution Center is involved in providing credentials to the client's machine which can be passed along to access the other strengthened machine).



Direct connections *from* the strengthened *to* the untrusted realm are allowed.

One-time passwords are used for direct connections from the untrusted to the

Untrusted to strengthened

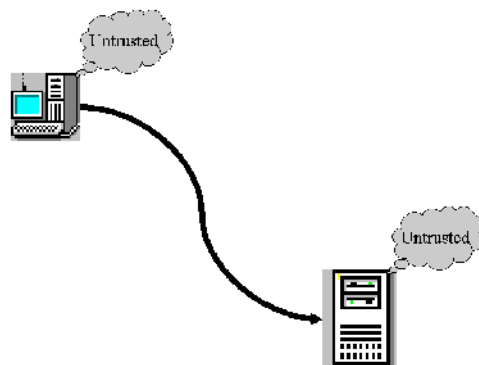


strengthened realm at Fermilab. Strengthened machines are configured to respond in *portal mode* when requests for access come from machines in the untrusted realm. In portal mode, the strengthened machine acts as a secure gateway into the strengthened realm, requiring a single-use password for authentication. This avoids transmission of reusable clear-text passwords over a potentially unprotected network.

Different programs exist for generating non-reusable passwords, and at Fermilab we currently support CRYPTOCARD (described in Appendix : *Using your CRYPTOCARD*). No special hardware or software is required on the untrusted system.

For connections between untrusted machines, strong authentication is not

Untrusted to untrusted



involved. The standard network programs are used in the normal way.

A.4 Features of Strong Authentication at Fermilab

The strong authentication model implemented at Fermilab:



- improves authentication and access control
- is adaptable to new computer security threats and changes in system security requirements and to new styles of computing
- is integrated with AFS (I.e., if your machine is part of the strengthened realm and it runs AFS, then when you log on and get Kerberos authentication, you also automatically get an AFS token.)
- is robust and stable
- can be readily deployed to collaborating universities and laboratories, including those outside the United States
- accommodates all the supported UNIX operating systems, as well as Windows and Macintosh systems¹
- is capable of establishing trust relationships with other institutions where similar strong authentication systems are in place, allowing each user to have a single identity (userid) encompassing multiple institutions
- provides meaningful improvements in security and authentication for the Run II experiments, and is incorporated into the Run II software infrastructure
- provides access for users and systems from outside the strengthened realm via the portal function, without the installation of special hardware or software on the users' desktops (this allows access via systems that do not or can not have strong authentication directly installed, e.g., a public terminal, a "dumb" X terminal, or a PalmPilot)

1. Certain systems, such as embedded systems or specialized on-line systems may not be capable of participating directly in strong authentication. These systems may be accommodated by alternate access.

